

# EEM Failover Setup

This was taken directly from the CA Embedded Entitlements Manager Getting Started Guide (Chapter 7)

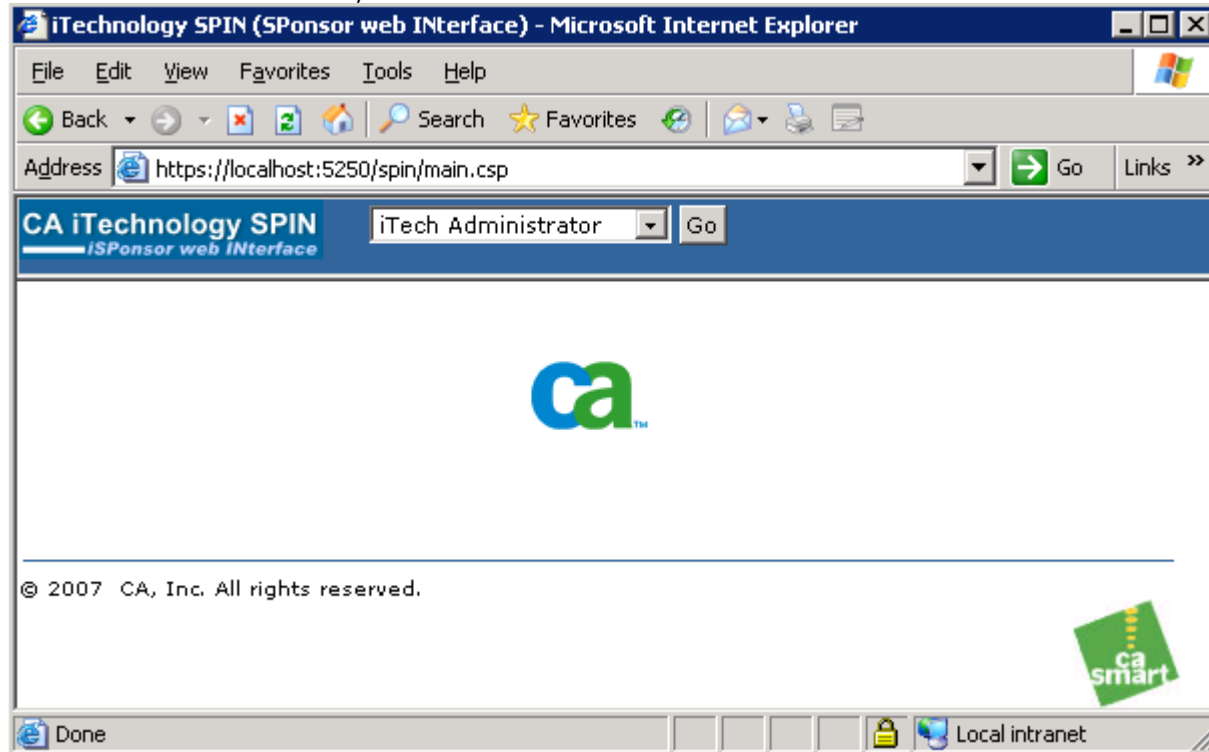
## CA EEM Server Failover

**Note:** Ensure you install the same version of CA EEM Server on both the server hosts (Server1 and Server2) and synchronize their system time.

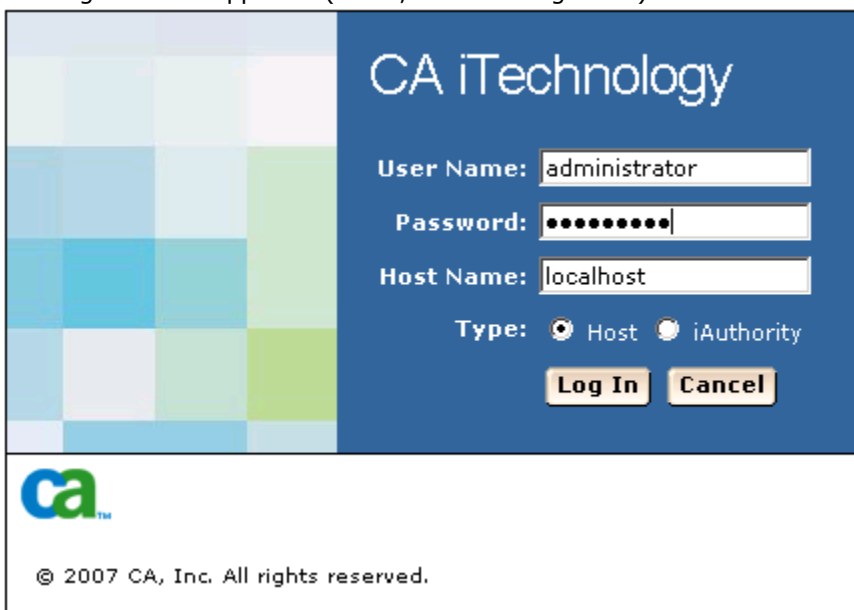
You can configure Server1 to trust the sessions and certificates of Server2.

### To configure server1 for failover

1. Enter the URL `https://server1:5250/spin`.
2. Select iTech Administrator, and click Go.



The Login screen appears. (if not, click the Login link)



3. Enter the login credentials as follows based on your selection of the option Type in the Login screen:

**Host**

Login as root or administrator.

**iAuthority**

Login as eiamadmin.

4. Click the Configure tab, add Server2 as Hostname in the Trusted iAuthority Hosts pane and click Trust. An entry is added in iControl.conf file and Server1 starts trusting sessions from Server2.

**Trust another iAuthority**  
• Hostname:



Host: localhost Welcome: administrator ( [Logout](#) )

Updated: Wed Jul 15 10:39:55 2009

Language:

Status

Configure

iAuthority

iRegistry

SPIN

**iControl Configuration**

**Start Time:** Tue Jul 14 13:41:26 2009  
**Events Received:** 2822  
**Event Plugin:**  
**Route Events:** false  
**Route Events Host:**  
**Events To Cache:** 100  
**Saf Directory:**  
**Saf Expiration:** 72  
**Max Events Per Second:**  
**Ignore Signature:** false  
**Credential Life Time:** 24

**Trusted iAuthority Hosts**

Host name	Remove
localhost	<input type="button" value="X"/>
server2	<input type="button" value="X"/>

**Trust another iAuthority**  
• Hostname:

5. Click the iAuthority tab, enter Label as Server2, browse to the location of PEM Certificate file in the Add Trusted Root pane and click Add Trusted Root.


**Note:** The PEM certificate file (rootcert.pem) is located in the iTechnology directory of Server2.

(x:\Program Files\CA\SharedComponents\iTechnology\rootcert.pem)

An entry is added in iAuthority.conf and Server1 starts trusting certificates from Server2.


**If you are using build 8.4 SP03 (build 8.4.216) or later use rootcert.cer file.**

## iAuthority Certificate Authentication Configuration

Label	Certificate	All Admin	Admin DN list	Remove
myself	<b>Issuer:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa6 <b>Subject:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa6	false		


**Add Trusted Root**

• **Label:**



• **PEM Certificate file:**  

• **All Admin:** ☐

• **Admin DN List:**




## iAuthority Certificate Authentication Configuration

Label	Certificate	All Admin	Admin DN list	Remove
myself	<b>Issuer:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa6 <b>Subject:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa6	false		
server2	<b>Issuer:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa2 <b>Subject:</b> O=iTechnology,OU=Configuration,OU=CertServer,CN=sidri01-qa2	false		


**Add Trusted Root**

• **Label:**

• **PEM Certificate file:**  

• **All Admin:** ☐

• **Admin DN List:**



You must also configure Server2 to trust the sessions and certificates of Server1.

### To configure server2 for failover (repeat steps above for Server2)

1. Enter the URL <https://server2:5250/spin>.
  2. Select iTech Administrator.
  3. Log in as root or administrator by selecting Host or as eiamadmin by selecting iAuthority.
  4. Click the Configure tab, add Server1 as Hostname in the Trusted iAuthority Hosts pane and click Trust. An entry is added in iControl.conf file and Server2 starts trusting sessions from Server1.
  5. Click the iAuthority tab, enter Label as Server1, browse to the location of PEM Certificate file in the Add Trusted Root pane and click Add Trusted Root.
- Note:** The PEM certificate file (rootcert.pem) is located in the iTechnology directory of Server1. An entry is added in iAuthority.conf and Server2 starts trusting certificates from Server1.

# Configure CA EEM Files

You must configure CA EEM Server1 to receive the list of available servers to fall back on, which are replicated versions.

## To configure CA EEM Server1

1. Open the iTechnology directory of Server1.

**Windows:** %IGW\_LOC%

**Linux and UNIX:** /opt/CA/SharedComponents/iTechnology (Default)

2. Open the iPoz.conf file and add the following tag: (C:\Program Files\CA\SharedComponents\iTechnology\iPoz.conf)  
<BackboneMember>Server2</BackboneMember>

3. Stop and start iGateway.

### Windows

```
net stop igateway  
net start igateway
```

### Linux and UNIX

```
/opt/CA/SharedComponents/iTechnology/S99igateway stop  
/opt/CA/SharedComponents/iTechnology/S99igateway start
```

You must also configure CA EEM Server2 to receive the list of available servers to fall back on, which are replicated versions.

## To configure CA EEM Server2

1. Open the iTechnology directory of Server2.

**Windows:** %IGW\_LOC%

**Linux and UNIX:** /opt/CA/SharedComponents/iTechnology (Default)

2. Open the iPoz.conf file and add the following tag: (C:\Program Files\CA\SharedComponents\iTechnology\iPoz.conf)  
<BackboneMember>Server1</BackboneMember>

3. Stop and start iGateway.

### Windows

```
net stop igateway  
net start igateway
```

### Linux and UNIX

```
/opt/CA/SharedComponents/iTechnology/S99igateway stop  
/opt/CA/SharedComponents/iTechnology/S99igateway start
```